UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,218	03/31/2004	Randolph L. Campbell	42P17825	6019

8791 7590 09/20/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
REZA, MOHAMMAD W	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
09/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/814,218	CAMPBELL ET AL.	
	Examiner	Art Unit	
	Mohammad W. Reza	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/31.2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/27/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are presented for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-8, and 23-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In these claims applicants mention, "a secure virtual machine monitor (SVMM) to implement the secure execution mode **in which a plurality of separate virtual machines are created**..... " which is generally narrative and indefinite with the invention. It is also controversy and conflicting with the other independent claims as claim 9, and 16. In these claims applicant mention, "**creating a secure execution environment in which a plurality of separate virtual machine operate**.....". Applicants do not point out clearly which limitations is the right way to define the present invention. According to the specification, limitations of claims 9, and 16 are the right way to represent the invention. In the first set of claims, the general interpretation of the limitation should be "plurality of separate virtual machines are created in a SVMM" whereas the second set of claims interpretation is "creating a secure environment in which a plurality of machines operate". So the way word "Create" has been used in these two sets claims arising the conflicting concept to each other.

The office will interpret these limitation with the regarding claims as best understood for applying the appropriate art for rejection purposes.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bugnion et al hereafter Bugnion (US patent 6496847) in view of Michael L. Spilo hereafter Spilo (US Patent 5459869).

4. As per claim 1, Bugnion discloses an apparatus comprising: a processor having a normal execution mode and a secure execution environment to create a secure execution environment (abstract, col. 8, lines 34-40); and a secure virtual machine monitor (SVMM) to implement the secure execution mode in which a plurality of separate virtual machines are created that operate simultaneously and separately from one another including at least a first virtual machine (col. 1, lines 56-59, col. Col. 4, lines 29-33) to implement trusted guest software in a protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in a non-protected memory area(col. 7, lines 15-40, col. 9, lines 12-22). Bugnion discloses the switching from secure virtual execution mode to normal execution mode (col. 7, lines 15-40, col. 9, lines 12-22). He does not expressly disclose wherein responsive to a

command to tear down the secure execution environment, the SVMM causes the processor to exit out of the secure execution mode, tears down the secure execution environment, and instructs the non-trusted guest OS to resume control in the normal execution mode. However, in the same field of endeavor, Spilo discloses wherein responsive to a command to tear down the secure execution environment, the SVMM causes the processor to exit out of the secure execution mode, tears down the secure execution environment, and instructs the non-trusted guest OS to resume control in the normal execution mode (abstract, col. 4, lines 7-25).

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Spilo's teachings of exit out of the secure execution mode and instruct the non-trusted OS to resume control with the teachings of Bugnion, for the purpose of suitably using switching mode conception to implement trusted guest software in a protected memory to a non-trusted guest system (abstract, col. 4, lines 7-25).

5. As per claim 2, Bugnion discloses The apparatus of claim 1, further comprising a virtual machine control structure (VCMS) to store guest state information related to the non-trusted guest operating system (OS) for use in restoring the non-trusted guest OS in the normal execution mode (col. 7, lines 15-40, col. 9, lines 12-22).

6. As per claim 3, Bugnion discloses the apparatus wherein the virtual machine control structure (VCMS) stores a guest OS entry point field to point to a command used for instructing the non-trusted guest OS to resume control at a virtual address (abstract, col. 8, lines 34-40). He does not discloses a host entry point field to point to a command

to instruct the processor to exit out of a virtual machine execution mode. However, Spilo discloses a host entry point field to point to a command to instruct the processor to exit out of a virtual machine execution mode (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 3.

7. As per claim 4, Bugnion discloses the apparatus comprising, the SVMM scrubbing the protected memory (abstract, col. 8, lines 34-40). He does not disclose associated with the trusted guest software when the secure execution environment is torn down. However, Spilo discloses associated with the trusted guest software when the secure execution environment is torn down (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 4.

8. As per claim 5, Bugnion discloses the apparatus comprising, the secure execution mode when the secure execution environment is torn down (abstract, col. 8, lines 34-40). He does not disclose the SVMM causing the processor to exit out of a virtual machine extension mode before exiting out. However, Spilo discloses the SVMM causing the processor to exit out of a virtual machine extension mode before exiting out (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 5.

9. As per claim 6, Bugnion discloses the apparatus wherein the non-trusted guest operating system (OS) (abstract, col. 8, lines 34-40). He does not disclose issues the

command to tear down the secure execution environment. However, Spilo discloses issues the command to tear down the secure execution environment (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 6.

10. As per claim 7, Bugnion discloses the apparatus wherein the secure virtual machine monitor (SVMM) issues the command (abstract, col. 8, lines 34-40). He does not disclose to tear down the secure execution environment. However, Spilo discloses to tear down the secure execution environment (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 7.

11. As per claim 8, Bugnion discloses the apparatus wherein the secure virtual machine monitor (SVMM) issues the command (abstract, col. 8, lines 34-40). He does not disclose to tear down the secure execution environment due to a detected security breach. However, Spilo discloses to tear down the secure execution environment due to a detected security breach (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 8.

12. As per claim 9, Bugnion discloses a method comprising: providing a normal execution mode in a processor and a secure execution mode in a processor (abstract, col. 8, lines 34-40); and creating a secure execution environment in which a plurality of separate virtual machines operate simultaneously and separately from one another

including at least a first virtual machine to implement trusted guest software (col. 1, lines 56-59, col. Col. 4, lines 29-33) in a protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in a non-protected memory area (col. 7, lines 15-40, col. 9, lines 12-22). Bugnion discloses the switching from secure virtual execution mode to normal execution mode (col. 7, lines 15-40, col. 9, lines 12-22). He does not expressly disclose wherein responsive to a command to tear down the secure execution environment, exiting out of the secure execution mode, tearing down the secure execution environment, and instructing the non-trusted guest OS to resume control in the normal execution mode. However, Spilo discloses wherein responsive to a command to tear down the secure execution environment, exiting out of the secure execution mode, tearing down the secure execution environment, and instructing the non-trusted guest OS to resume control in the normal execution mode (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 9.

13. As per claim 11, Bugnion discloses the method comprising: storing a guest OS entry point field to point to a command used for instructing the guest OS to resume control at a virtual address (abstract, col. 8, lines 34-40. He does not expressly disclose storing a host entry point field to point to a command to instruct the processor to exit out of a virtual machine execution mode (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 11.

14. Claims 10, and 12-15 are listed all the same elements of claim 2, and 4-8 but in method form rather than apparatus form. Therefore, the supporting rationales of the rejection to claim 2, and 4-8 apply equally as well to claim 10, and 12-15.

15. As per claim 16, Bugnion discloses a machine-readable medium comprising: providing a normal execution mode in a processor and a secure execution mode in a processor (abstract, col. 8, lines 34-40); and creating a secure execution environment in which a plurality of separate virtual machines that operate simultaneously and separately from one another including at least a first virtual machine to implement trusted guest software (col. 1, lines 56-59, col. Col. 4, lines 29-33) in a protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in a non-protected memory area (col. 7, lines 15-40, col. 9, lines 12-22). He does not expressly disclose wherein responsive to a command to tear down the secure execution environment, exiting out of the secure execution mode, tearing down the secure execution environment, and instructing the non-trusted guest OS to resume control in the normal execution mode. However, Spilo discloses wherein responsive to a command to tear down the secure execution environment, exiting out of the secure execution mode, tearing down the secure execution environment, and instructing the non-trusted guest OS to resume control in the normal execution mode (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 16.

16. As per claim 18, Bugnion discloses the machine readable medium comprising: storing a guest OS entry point field to point to a command used for instructing the guest OS to resume control at a virtual address (abstract, col. 8, lines 34-40. He does not expressly disclose storing a host entry point field to point to a command to instruct the processor to exit out of a virtual machine execution mode (abstract, col. 4, lines 7-25). The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 18.

17. Claims 17, and 19-22 are listed all the same elements of claim 2, and 4-8 but in machine readable medium form rather than apparatus form. Therefore, the supporting rationales of the rejection to claim 2, and 4-8 apply equally as well to claim 17, and 19-22.

18. As per claim 23, Bugnion discloses a system comprising: a processor including virtual machine extension (VMX) instruction support (abstract, col. 8, lines 34-40), the processor further having a normal execution mode and a secure execution mode to create a secure execution environment (col. 1, lines 56-59, col. Col. 4, lines 29-33); a memory including a protected memory area and a non-protected memory area (col. 7, lines 15-40, col. 9, lines 12-22); and a secure virtual machine monitor (SVMM) to implement the secure execution environment in which a plurality of separate virtual machines are created that operate simultaneously and separately from one another including at least a first virtual machine to implement trusted guest software in the protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in the non-protected memory area (col. 1, lines 56-59, col. Col.

4, lines 29-33). He does not expressly disclose wherein responsive to a command to tear down the secure execution environment, the SVMM causes the processor to exit out of the secure execution mode, tears down the secure execution environment, and instructs the non-trusted guest OS to resume control in the normal execution mode. However, Spilo discloses wherein responsive to a command to tear down the secure execution environment, the SVMM causes the processor to exit out of the secure execution mode, tears down the secure execution environment, and instructs the non-trusted guest OS to resume control in the normal execution mode (abstract, col. 4, lines 7-25).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 23.

19. Claims 24-30 are listed all the same elements of claim 2-8 but in system form rather than apparatus form. Therefore, the supporting rationales of the rejection to claim 2-8 apply equally as well to claim 24-30.

Conclusion

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/17/07